ILUSTRE
COLEGIO DE ABOGADOS
DE MADRID

10 CONSEJOS BÁSICOS PARA LA ADECUACIÓN AL RGPD

Orientaciones y consejos básicos para la adecuación de la actividad de un abogado al Reglamento General de Protección de Datos y el cumplimiento de éste.

1. Analiza qué datos de carácter personal tratas en el ejercicio profesional y con qué finalidades concretas. Un abogado o despacho puede tratar datos como responsable, entre otras actividades, para la:

- Gestión profesional del asesoramiento y defensa jurídica.
- Gestión de recursos humanos y laborales.
- Gestión económica y fiscal.
- Gestión de un blog y una página web.
- Gestión de las obligaciones del propio Reglamento General de Protección de Datos (ejercicio de derechos, notificación de brechas de seguridad), etc.

Identifica también en qué relaciones tratas datos como encargado del tratamiento, en las que otros son los responsables. Un abogado o despacho puede tratar datos como encargado del tratamiento, entre otras actividades, para la:

- Colaboración con otros abogados, despachos, o empresas.
- Prestación de servicios de asesoría/gestoría empresas (p.ej. gestión de nóminas), etc.

2. Analiza los riesgos que pueden afectar al tratamiento de datos. En especial los riesgos que pueden afectar a:

- La integridad de los datos (modificación o alteración).
- La disponibilidad de los datos personales (pérdida o borrado).
- La confidencialidad de los datos (acceso no autorizado).
- El ejercicio de los derechos (ausencia de procedimientos).
- Los principios relativos al tratamiento (ausencia de legitimidad para el tratamiento; tratamiento ilícito), etc.

Determina las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado en función de los riesgos detectados.

La Agencia Española de Protección de Datos tiene disponible una Guía Práctica de Análisis de Riesgos y de medidas básicas de seguridad:

https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/2018/AnalisisDeRiesgosRGPD.pdf

Los riesgos identificados y las medidas de control definidas deben documentarse.

3. Una vez identificadas las actividades para las que tratas datos de carácter personal y las medidas de seguridad apropiadas para los riesgos identificados, **elabora el Registro Actividades del Tratamiento** como responsable del tratamiento (y, en su caso, como encargado del tratamiento).

Debe contener la siguiente información

- Identidad del responsable (o del encargado)
- Nombre de la actividad
- Base jurídica o legitimación para el tratamiento
- Fines del tratamiento
- Colectivo de interesados de los que se tratan datos
- Categorías de datos que se tratan.
- Categoría destinatarios, a los que se ceden o comunican datos
- Transferencias internacionales que, en su caso, se realicen
- Plazo de conservación o supresión de los datos
- Medidas de seguridad

Guarda y actualiza periódicamente este registro de actividades. Este registro de actividades no se comunica a la Agencia Española de Protección de Datos (AEPD), quedando en todo caso a su disposición por si los solicitara. Con el RGPD desaparece la obligación de inscribir los ficheros ante la AEPD.

4. **Identifica qué empresas te prestan servicios y tienen acceso a datos de carácter personal** de los que eres responsable. A un abogado o despacho le pueden prestar servicios y tener acceso a datos como encargados del tratamiento:

- Otros abogados o despachos colaboradores.
- Prestadores de servicios informáticos.
- Proveedores de correo electrónico, página web, o de servicios en la nube.
- Gestorías fiscales o laborales, etc.

Formaliza un contrato con los encargados del tratamiento.

La Agencia Española de Protección de Datos ha elaborado unas Directrices para la elaboración de estos contratos:

https://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/directricescontratos.pdf

5. Analiza por qué vía te llegan los datos de carácter personal. **Tendrás que informar al interesado de que tratas sus datos.**

La Agencia Española de Protección de Datos ha elaborado una Guía para cumplir con el deber de informar:

https://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/modelocl ausulainformativa.pdf

Es aconsejable que en la formalización de la relación con el cliente, en la hoja de encargo o contrato le informes del tratamiento de sus datos y de sus derechos. La relación contractual legitima el tratamiento de los datos del cliente. Si además de para el encargo profesional, tratas los datos del cliente para otras finalidades recaba en la hoja de encargo o contrato el consentimiento expreso para ello,

Si el cliente es un cliente de justicia gratuita o de Turno de Oficio también le tendrás que informar del tratamiento de sus datos y de sus derechos. La designación legitima el tratamiento de los datos del cliente (arts. 6.1. c y e RGPD y Ley 1/1996, de 10 de enero, de asistencia jurídica gratuita).
Si recabas datos a través de una web, en formularios de primera consulta o contacto, tendrás que informar debidamente al interesado y obtener su consentimiento.

Te corresponderá, en su caso, probar como responsable que has informado al interesado. Es aconsejable que la información se proporcione por escrito y a ser posible recabando prueba de haber informado o de la voluntad o consentimiento del interesado.

6. Recuerda que si no hay otra habilitación para tratar los datos (contrato, cumplimiento de obligación legal, etc.) necesitarás el consentimiento inequívoco del interesado para tratar sus datos. Salvo en categorías de datos de categorías especiales, donde ha de ser explícito, el consentimiento puede otorgarse de forma implícita cuando se deduzca de una acción del interesado (por ejemplo, cuando el interesado continúa navegando por una web y acepta así el que se utilicen cookies para monitorizar su navegación).

Los tratamientos iniciados con anterioridad al inicio de la aplicación del RGPD sobre la base del consentimiento seguirán siendo legítimos siempre que ese consentimiento se hubiera prestado del modo en que prevé el propio RGPD, es decir, mediante una manifestación o acción afirmativa.

El RGPD no admite formas de consentimiento tácito o por omisión, que se basan en la inacción.

7. Recuerda que la normativa de protección de datos personales no puede analizarse en un contexto aislado sino que deben tenerse en cuenta, entre otras cuestiones, los deberes propios de la función profesional, del ejercicio del derecho de defensa y, en especial, el secreto profesional.

Prevalece el derecho a la defensa del cliente frente a los derechos de protección de datos de la parte contraria o contraparte:

- No hace falta consentimiento para tratar datos de la contraparte.
- El secreto profesional impide conceder el acceso a la contraparte a los datos que se tratan de ella o a otros interesados de los que el abogado haya conocido en el ejercicio de su actividad en el ejercicio del derecho de defensa. En aquellos supuestos en los que se estén tratando datos personales relativos a la contraparte en un proceso judicial, el abogado debe atender el ejercicio de los derechos de acceso y cancelación. Si bien esos ejercicios de derechos deben ser desestimados por el abogado, de acuerdo con dicha prevalencia del derecho de defensa y el secreto profesional que contribuye a su realización.

8. Los abogados y despachos de abogados deben valorar la necesidad de designar un Delegado de Protección de Datos (DPD).

El nombramiento de un Delegado de Protección de Datos es obligatorio, entre otros supuestos, para "el tratamiento a gran escala de categorías especiales de datos o datos personales relacionados con condenas y delitos penales."

No se considera tratamiento a gran escala el tratamiento por un abogado que ejerce individualmente, por lo que los abogados que ejercen de forma individual no tendrán que nombrar Delgado de Protección de Datos.

El Grupo de Trabajo del Artículo 29 (GT 29) - órgano consultivo independiente integrado por las Autoridades de Protección de Datos de todos los Estados miembros, el Supervisor Europeo de Protección de Datos y la Comisión Europea - ha elaborado unas Directrices sobre los Delegados de Protección de Datos. Disponibles en:

https://www.agpd.es/portalwebAGPD/canaldocumentacion/docu_grupo_trabajo/wp29/common/Traduc_oficial_ult_version/wp243rev01_es.pdf

Si concluyes que no necesitas designar Delegado de Protección de Datos, justifícalo y documéntalo.

9. Los abogados y despachos de abogados deben valorar la necesidad de realizar una Evaluación de Impacto de Protección de Datos (EIPD).

La realización de una EIPD es obligatoria cuando el tratamiento "entrañe probablemente un alto riesgo para los derechos y libertades de las personas físicas".

Aunque en otras circunstancias pueda requerirse una EIPD, el artículo 35 RGPD, apartado 3 ofrece algunos ejemplos de cuando una operación de tratamiento "es probable que entrañe un alto riesgo". Entre los supuestos contemplados está el tratamiento a gran escala de las categorías especiales de datos o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo.

No se considera tratamiento a gran escala el tratamiento por un abogado que ejerce individualmente, por lo que los abogados que ejercen de forma individual no tendrán que realizar Evaluación de Impacto de Protección de Datos.

El GT 29 ha elaborado unas Directrices sobre la EIPD y para determinar si el tratamiento "entraña probablemente un alto riesgo" a efectos del Reglamento (UE) 2016/679. Está disponible en:

https://www.agpd.es/portalwebAGPD/canaldocumentacion/docu_grupo_trabajo/wp29/common/Traduc_oficial_ult_version/wp248_rev.01_es.pdf

La Agencia Española de Protección de Datos ha elaborado una Guía Práctica de EIPD. Disponible en:

https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/2018/Guia_EvaluacionesImpacto.pdf

Si concluyes que no necesitas realizar EIPD, justifícalo y documéntalo.

10. **Como regla general, cuando se produzca una violación de la seguridad de los datos, el responsable debe notificarla a la Agencia Española de Protección de Datos.** La notificación de la quiebra a las autoridades debe producirse sin dilación indebida y, a ser posible, dentro de las 72 horas siguientes a que el responsable tenga constancia de ella. Deben documentarse todas las violaciones de seguridad.

En los casos en que sea probable que la violación de seguridad entrañe un alto riesgo para los derechos o libertades de los interesados, hay que notificar también a éstos.

Finalmente, recuerda que la Agencia Española de Protección de Datos ha elaborado y recopilado una serie de documentos y guías útiles para la adecuación al RGPD y su cumplimiento. Están disponibles en la web de la Agencia: www.agpd.es.

En este documento se contiene un listado para evaluar el cumplimiento del RGPD:

https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/2018/LISTADO_DE_CUMPLIMIENTO_DEL_RGPD.pdf

En caso de duda puedes plantear una consulta a la Agencia en la sede electrónica de la web.